Securing Your Home Wireless Network

20140228

Securing Your Home Wireless Network— Do's and Don'ts

- When creating passwords for your networks devices, ensure that they are sufficiently long and complex by using uppercase letters, lower-case letters, numbers, and symbols. Consider a multi-password phrase that does not consist of dictionary-based words. An example of a satisfactorily long and complex password would be ILuvF00tb@77 from the phrase "I love football."
- Use a cable to directly access the internet for any computers that remain stationary.
- Turn off your wireless network when you will not be using it for an extended period of time.
- If you have guest access set up for your network, ensure that it is password protected.
- If possible, turn on automatic updates for your network device's firmware. If automatic updates are not offered, periodically check for firmware updates on the network devices' websites and manually download and install them.
- If your router is compromised or if you cannot remember the password, you can restore it to the default factory settings by pressing the reset button located on the back of the router.
- Position the router away from windows and further into the interior of your house to decrease the reach of the signal.

Glossary of Commonly Used Terms

Wireless Router - Physical hardware that allows users to connect their devices to a shared internet network.
Service Set Identifier (SSID) - The public name of a wireless network.
Wired Equivalent Privacy (WEP) - Older security algorithm for wireless networks that has numerous security flaws.
Wi-Fi Protected Access (WPA) - More recent security algorithm for wireless networks. Also has many security flaws.
Wi-Fi Protected Access II (WPAZ) - The most secure algorithm for wireless networks. Improved upon and replaced WPA.
Pre-shared key (PSK) - An authentication mechanism that mandates a password. Adds additional security to wireless networks.
Hypetext Transfer Protocol (HTTP) - Protocol for communication over a computer network.
Hypertext Transfer Protocol Secure (HTTPS) - Uses various encryption protocols to add additional security to HTTP.
Media Access Control (MAC) Address - A unique, individual identifier assigned to computers and devices.

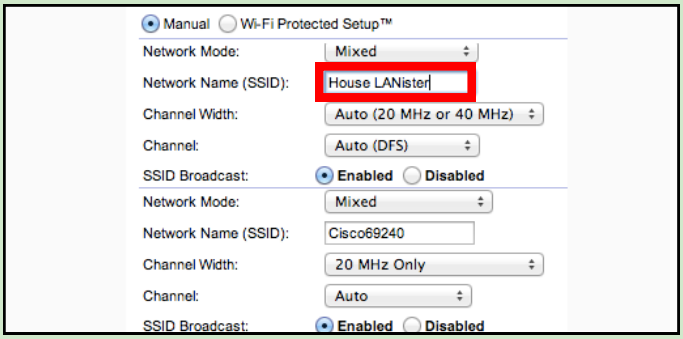
Access Your Router

To access your router, you must enter the appropriate IP address, username, and password. Most routers share similar log-in information

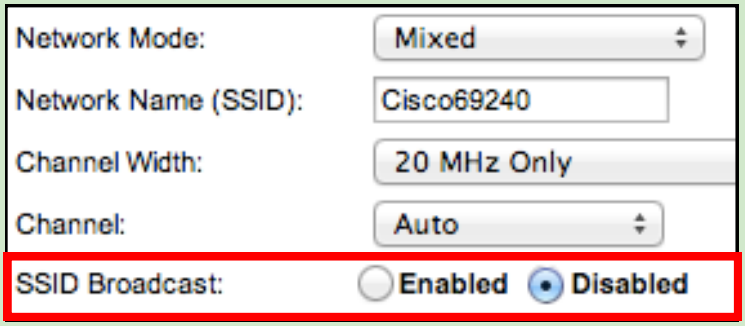
Router	IP Address	Username	Password
3Com	192.168.1.1	n/a	admin
Apple	192.168.1.1	admin	admin
Asus	192.168.1.1	admin	admin
Belkin	192.168.2.1	admin	n/a
Dell	192.168.1.1	n/a	admin
Linksys	192.168.0.1	admin	admin
Medialink	192.168.0.1	n/a	admin
Motorola	192.168.100.1	admin	motorola
Netgear	192.18.0.1	admin	password
TP-LINK	192.168.1.1	admin	admin
US Robotic	192.168.1.1	admin	admin

Choose a username that does not include you or your family's names and a password that is long and complex.

Creating a Unique SSID



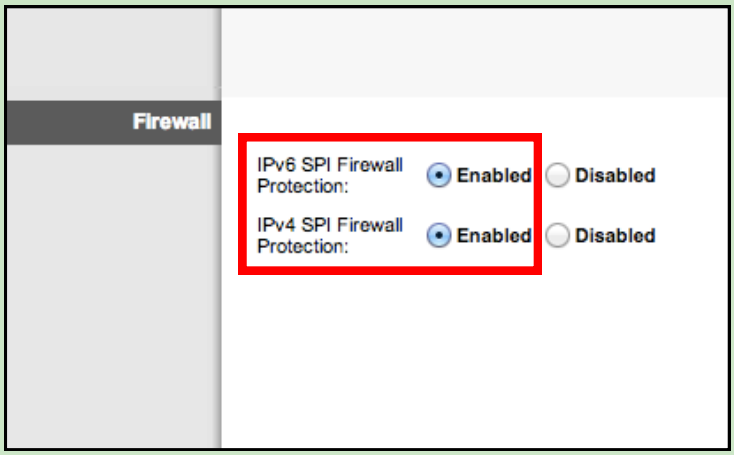
Disabling the SSID Broadcast



Securing Your Home Wireless Network

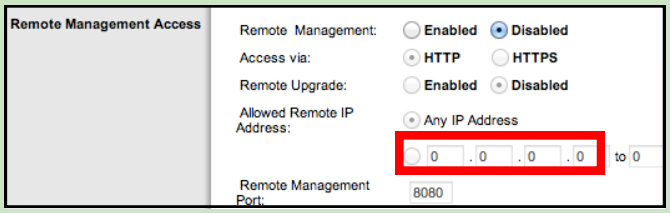
20140228

Router Firewall

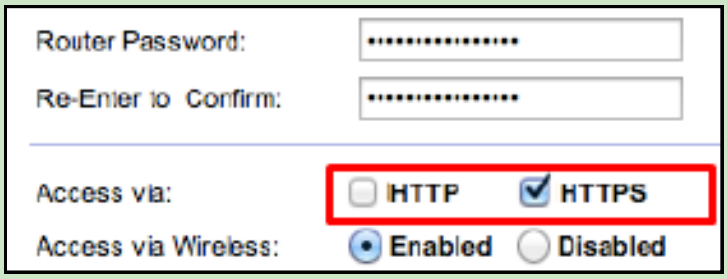


Remote Access

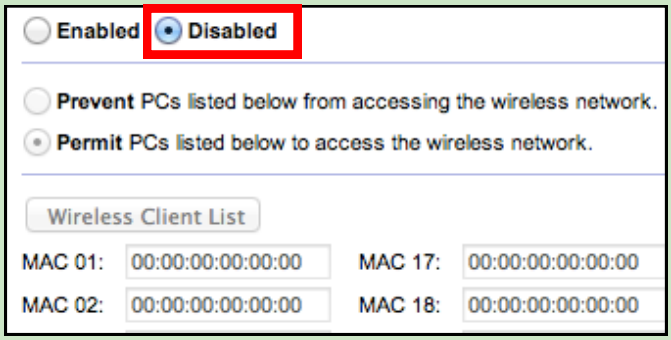
Check that the Remote Management IP Address is set to **0.0.0.0** in order to ensure that remote access is disabled.



Enabling HTTPS



Wireless MAC Filtering



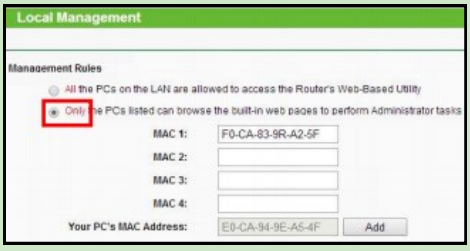
Enable MAC address filtering to ensure that only approved computers and devices can connect to your router

Adding MAC Addresses

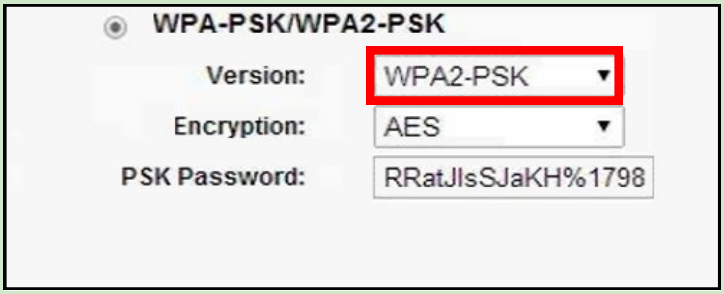
Enter the Mac address and a brief description of the connected device.

Wireless MAC Filtering

Restricting administrative access through the web to specific devices. Add the MAC addresses of each computer and device you wish to add.



Encryption



Between the optional WEP, WPA, WPA-PSK, WP2, and WPA2-PSK algorithms, you should select WPA2-PSK and also AES for encryption. The PSK password should be long and complex, but different than the administrative router access password.

Useful Links

Practically Networked	http://www.practicallynetworked.com/support/wireless_secure.htm
Wi-Fi.org	www.wi-fi.org/discover-wi-fi/security
NIST	http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf